WRITTEN STATEMENT OF

STEVEN P. BANDY

MANAGER, CORPORATE SAFETY & SECURITY

MARATHON ASHLAND PETROLEUM

ON BEHALF OF THE

NATIONAL PETROCHEMICAL & REFINERS ASSOCIATION (NPRA)
&
THE AMERICAN PETROLEUM INSTITUTE (API)

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
OF THE
HOUSE COMMITTEE ON HOMELAND SECURITY

HEARING ON PREVENTING TERRORIST ATTACKS ON AMERICA'S CHEMICAL PLANTS

June 15, 2005

Introduction

Good morning, Mr. Chairman, Ranking Member Sanchez, and Members of the Committee. I want to thank the Committee for holding this important hearing today. I look forward to discussing how the refining and petrochemical industries are performing the critical task of maintaining and strengthening the security of our national energy and petrochemical infrastructure.

I am the Manager of Corporate Safety & Security for Marathon Ashland Petroleum LLC (MAP), headquartered in Findlay, Ohio. As Manager of Corporate Security for MAP, I am responsible for ensuring the secure operations of our facilities for our employees, customers and the communities in which we operate. MAP is a refining, marketing and transportation company, with a complementary network of operations stretching across 21 states. We own and operate seven refineries and have a total crude oil capacity of approximately 948,000 barrels per day.

Today I am testifying on behalf of NPRA, the National Petrochemical & Refiners Association and API, the American Petroleum Institute. NPRA has more than 450 member companies, including virtually all U.S. refiners and petrochemical manufacturers, their suppliers and vendors. Petrochemical companies use processes similar to those in a refinery. NPRA companies supply consumers with a wide variety of products used daily in their homes and businesses. These products include gasoline, diesel fuel, home heating oil, jet fuel, lubricants, and the chemicals that serve as building blocks for everything from plastics to clothing to medicine to computers. API, a national trade association for the U.S. oil and natural gas industry, represents all sectors of the industry, including exploration, transportation, refining, storage, distribution and marketing.

Overview/Summary of Statement

Maintaining the security of our workforce, plant, property, and equipment has always been a priority at refineries and petrochemical plants. Refiners and petrochemical manufacturers are heavily engaged – and were so even before September 11 – in maintaining and enhancing security. These industries have long operated globally, often in unstable regions overseas where security is an integral part of providing for the world's energy and petrochemical needs. NPRA and API member companies continue to address and prepare for potential threats to our facilities. We are absolutely committed to keeping all sites as secure as possible from threats of violence or terrorism. We are keenly aware of the responsibility we have to our employees, to our customers, and to the communities in which we operate. We have been working diligently to strengthen the security of our facilities, and in my testimony today I will outline some of the actions we have taken.

When the tragic events of September 11, 2001, occurred, we as a nation realized immediately that a vastly different set of threats had to be taken into consideration in order to protect our homeland. The refining and petrochemical industries were no different. Industry – and I say this with special emphasis – did not wait for new government regulations before implementing additional and far-reaching facility security

measures to address these new threats. Industry consulted with and obtained the input of federal, state, and local agencies, first responders and other security experts who are knowledgeable about the strategy, tactics and plans employed by terrorists. That information, coupled with the knowledge that each company has about the specifics of its own technology and materials, was then used to conduct intensive security vulnerability assessments. Based on those assessments, detailed facility security plans were prepared and implemented.

Refiners and petrochemical manufacturers have taken and will continue to take additional measures to ensure facility security. We have developed close, working relationships with key federal agencies and state and local law enforcement offices to exchange critical infrastructure information. We have held joint training exercises simulating actual terrorist attacks and have developed educational programs featuring federal and state government officials with security expertise. We have sponsored association meetings to share best industry practices. This affords companies the opportunity to learn what others are doing, discuss new approaches and ideas, and implement the approaches that best fit their own particular security needs.

With those considerations as background, NPRA and API urge the Committee to consider the following comments regarding the current state of security-related activities at refining and petrochemical facilities:

- The refining and petrochemical industry will continue to maintain and improve our security operations to protect the vital network that provides a reliable supply of fuels and other petroleum and petrochemical products needed to keep our nation strong and our economy growing.
- Industry, in cooperation with government security agencies, has reassessed security vulnerabilities and implemented strong and effective security measures since September 11, 2001.
- Industry complies with security requirements under post 9-11 federal security law, such as the Maritime Transportation Security Act and the Patriot Act.
- A strong working relationship has been established between government security agencies and the refining and petrochemical industry to exchange “real-time” intelligence data on security issues that allows them to respond rapidly to terrorist threats.
- Industry has partnered with the Department of Homeland Security on many important security initiatives and programs, including the Risk Assessment Methodology for Critical Asset Protection, or RAMCAP, the Homeland Security Information Network (HSIN), and Buffer Zone Protection Plans. (These will be discussed in more detail in my statement.)
- Industry supports full compliance with existing security regulations, adequate funding for DHS and other security agencies, and continuing public-private partnership efforts to protect facilities and vessels and strengthen intelligence-sharing networks.
- Congress has been wise to restrict public release of facility specific security information, the release of which would be disruptive to ongoing security operations.

Industry has conducted facility security vulnerability assessments.

In 2003, NPRA and API, working with other industry groups, the Department of Homeland Security and the Department of Energy, developed and provided industry with a peer-reviewed security vulnerability assessment (SVA) methodology. In 2004, industry expanded the SVA methodology to include transportation-related activities, including pipelines and rail and truck transportation. DHS has endorsed the vulnerability assessment methodology and uses it to train its employees.

The security vulnerability assessment methodology is a sophisticated and effective tool used to identify the security hazards, threats and vulnerabilities of a facility, and to evaluate the best measures to provide safe operations for employees and the public. The methodology provides the framework for a complete security analysis of the facility and its operations. Depending on the type and size of the facility, the assessment utilizes expertise in physical and cyber security, process safety, facility and process design and operations, emergency response, management, law enforcement, and other disciplines as necessary.

Differences in geographic location, type of operations, and on-site quantities of hazardous substances all play a role in determining the approach taken. Security vulnerability assessments typically include the following types of activities:

- Characterizing the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
- Identifying and characterizing threats against those facilities and evaluating them in terms of their attractiveness as targets for various adversaries, along with the consequences if these assets are damaged or stolen;
- Identifying potential security vulnerabilities that threaten the asset's service or integrity;
- Determining the risk represented by these events or conditions by evaluating the likelihood of a successful event and the consequences of an event if it were to occur; and
- Making specific recommendations for incident mitigation and countermeasures appropriate to the risk level.

Based on the results of the security vulnerability assessment, companies identify appropriate security measures and incorporate them in security plans which are then implemented.

Companies comply with security requirements under the Maritime Transportation Security Act of 2002.

A majority of the almost 150 refineries and 200 petrochemical manufacturing facilities in the United States are subject to the jurisdiction of the U.S. Coast Guard, and are therefore regulated pursuant to the security requirements of the Maritime Transportation Security Act (MTSA) of 2002. (See attached map of U.S. refineries.) The Act requires that these facilities conduct security vulnerability assessments and submit

comprehensive security plans to the U.S. Coast Guard. These security plans were submitted by facilities in December 2003. They were reviewed and approved by the Coast Guard in 2004. Under the Maritime Transportation Security Act, companies are also required to designate facility security officers to oversee the implementation of their security plans. This officer is required to conduct drills on a quarterly basis to test elements of the facility's security plan. We understand that the Coast Guard has been pleased with the petroleum and petrochemical industry's implementation of the Act.

Industry has implemented strong, new security measures since September 11.

Media reports sometimes leave the impression that the industry has not taken any new security initiatives since September 11. That simply is not true. With the critical information gained from conducting their security vulnerability assessments, facilities have taken the following specific measures to enhance security:

- Reconfigured sites allowing critical assets to be set back from the perimeter.
- Installed sophisticated, state-of-the-art electronic intrusion detection systems around our perimeters and on buildings.
- Implemented card-access controls with new biometric technology readers, such as retina or thumbprint scanners.
- Acquired enhanced security communication systems.
- Shared security response plans with local law enforcement and appropriate federal agencies.
- Conducted drills and exercises to test security and response plans.
- Hired additional security personnel to assist in our security efforts, which are an around the clock, seven days per week priority.

I emphasize that this is just a partial list. A longer list of measures taken by our industry is included as an attachment to this statement, but it, too, is only a partial list of measures taken as a result of a dynamic process.

Industry sponsors educational programs and holds training exercises with government officials to enhance security at facilities.

NPRA and API have established standing committees on security; I am a past Chairman of the NPRA Security Committee and play an active role in the API Security Committee. NPRA has held or co-sponsored more than a dozen facility security conferences and workshops, featuring federal and state policymakers, security and counterterrorism experts, and the sharing of best practices. In February of this year, for example, NPRA conducted an intensive training workshop for persons designated as Facility Security Officers under the Maritime Transportation Security Act. The workshop enabled them to better fulfill their responsibilities under MTSA. Since 2002, API has been hosting training sessions for industry and government personnel to teach them how to use the vulnerability assessment methodology and develop security plans.

NPRA has held two training exercises in cooperation with Texas Homeland Security. The exercises were conducted by Texas A&M University's National Emergency Response and Rescue Training Center and Texas Engineering Extension Service. The most recent training exercise, "Safe Horizon," was held in March of this year. This exercise was focused on incident deterrence and prevention of a postulated terrorist attack. These training exercises and educational programs provide information that allows companies to better assess the effectiveness of their own security policies, plans, and procedures, and make modifications as necessary.

In addition to the SVA Methodology, API developed the first edition of "Security Guidelines for the Petroleum Industry" in March 2002. It has since been revised and the third edition was released in April 2005. These Guidelines provide general guidance for effectively managing security risks and provide a reference to federal security laws and regulations impacting petroleum operations. I would like to provide a copy of both guidance documents, the SVA methodology, "API/NPRA Security Vulnerability Assessment Methodology for the Refining and Petrochemical Industries" and the "Security Guidelines" to the Committee and request that they be included as part of the hearing record.

Industry works with federal, state and local officials to enhance facility security.

The success of security programs in the refining and petrochemical industries is due in large part to the excellent working relationships our industry has established with various federal, state, and local governmental agencies. NPRA, API and their member companies work with more than a dozen federal agencies, as well as state and local law enforcement agencies and emergency responders throughout the nation to share critical infrastructure information and receive updates on the latest intelligence about terrorist focus and targets. The agencies that we work with include the FBI, the Department of Transportation, the Department of Energy, the Department of Defense, the CIA, the Government Accountability Office, and, of course, the Department of Homeland Security and its various components, including the U.S. Secret Service, the Transportation Security Agency, and the U.S. Coast Guard.

Our relationship with DHS and other security agencies allows immediate access by government and industry to rapidly changing information affecting facility security. These relationships and communications are essential in keeping our facilities secure. If an agency is turned into an industry regulator through enactment of federal security legislation, the dynamics of the relationship will undoubtedly change and this level of information sharing could be diminished.

The American Petroleum Institute has worked with our state petroleum councils to disseminate the API Security Guidelines to assist their state agencies in preparing plans to upgrade security at our facilities across the nation. As an example, in New Jersey where the industry has considerable presence with six refineries and many terminals, former Governor McGreevey accepted the API Security Guidance as the state's accepted petroleum industry practices in October of 2003. Since then, the New Jersey Petroleum

Council supplemented by company experts has been involved in educating state and local officials in security issues through regular meeting and training seminars.

Industry is working with DHS to improve risk assessment and to develop buffer zone protection plans.

Our members are working with DHS on the RAMCAP, or Risk Assessment Methodology for Critical Asset Protection, project. This approach to risk assessment and management will provide a consistent framework for the assessment, reporting and management of terrorism risks across the nation's critical infrastructure and key resources. This will be accomplished by developing a common risk-based method for comparing security risks, thereby giving Congress and the executive branch the tools they need to make decisions and allocate resources based on risk. In short, RAMCAP aims to put all infrastructures and key resources, including refineries and petrochemical plants, on a common risk platform.

Our members are also working with DHS, states, and local officials to protect and secure areas surrounding our facilities, which they neither own nor control, by developing buffer zone protection plans. These plans will identify specific threats and vulnerabilities with the buffer zone, analyze and categorize the level of risk, and recommend corrective measures to local law enforcement to reduce the risk of a terrorist attack.

Industry participates in private and public information networks to enhance security.

As stated earlier, information sharing is a vital part of our industry's security efforts, and so our NPRA and API members serve on several security-related public and private sector boards and task forces. These include participation on the Boards of the Energy Information Sharing & Analysis Center, or ISAC; the Oil & Natural Gas Sector Homeland Security Coordinating Council; and the Chemical Sector Coordinating Council. NPRA also serves on a working group of the Homeland Security Advisory Council (HSAC), helping to resolve legal impediments that hinder the submission of private sector information to government officials. NPRA and API members have also responded positively to a request to serve on a working group of the President's National Infrastructure Advisory Council.

One particularly important initiative underway – again, as a cooperative effort between DHS and industry - is the creation and implementation of the Homeland Security Information Network, or HSIN, for the petroleum and chemical industries. HSIN is an information sharing system facilitated by the DHS in partnership with the critical sector organizations. It links owners and operators with each other and with DHS and FBI to enable collaboration in protecting critical resources and to address physical and cyber threats, vulnerabilities, and incidents, and to share information about potential protective measures and best practices.

Chemical security legislation would be counter-productive.

To conclude, Mr. Chairman, refiners and petrochemical manufacturers take very seriously their responsibilities for not just maintaining, but strengthening security at their facilities to meet any new threats. Our industry has complied with modernized, post 9-11 federal security requirements. We have utilized expert engineers who understand our facilities better than any one else to conduct vulnerability assessments and implement new measures to protect against new threats. We have called upon experts throughout all of industry, government agencies, and the security business to capture the best practices to protect our facilities. And perhaps most importantly the industry has created an outstanding working relationship with government security agencies to rapidly receive the fast moving information needed to fight terrorism. This working partnership has been very effective in exchanging information to allow the industry to focus on the security threats that exist today and are most relevant. We look forward to continuing this security partnership. Our efforts show that industry does not need to be prodded by government mandates to take aggressive and effective steps to secure its facilities. In fact, industry is concerned that changing the nature of the existing relationship between DHS, other security agencies and industry could disrupt the open exchange and rapid response to threats that we have achieved to date. As a result, we are not advocating chemical security legislation because the existing system is working well, and, being a dynamic process, will continue to improve with time ..

In closing, I want to stress once again that NPRA and API member companies are absolutely committed to the security of our facilities. Thank you and I will be happy to answer any questions you may have.